(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
10 juillet 2003 (10.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/056750 A2

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR02/04502

(22) Date de dépôt international :
20 décembre 2002 (20.12.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/16950 27 décembre 2001 (27.12.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ARDITTI MODIANO, David** [FR/FR]; 46ter, rue Paul Vaillant-couturier, F-92140 Clamart (FR). **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 14, rue Emile Dron, F-81100 Flers (FR).

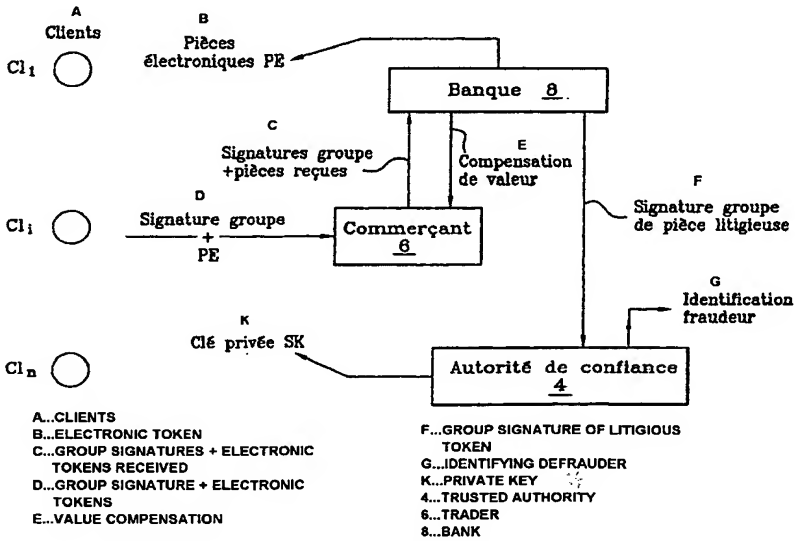
(74) Mandataires : **SOMNIER, Jean-Louis** etc.; Cabinet Ballot, 122, rue Edouard Vaillant, F-92593 Levallois-Perret Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) Title: CRYPTOGRAPHIC SYSTEM FOR GROUP SIGNATURE

(54) Titre : SYSTEME CRYPTOGRAPHIQUE DE SIGNATURE DE GROUPE



(57) **Abstract:** The invention concerns a system enabling a member (M) of a group (G) to produce, by means of customized data (z; K), a message (m) accompanied by a signature (8) proving to a verifier that the message originates from a member of the group (G). The invention is characterized in that the customized data is in the form of an electronic physical medium (26). Advantageously, the latter also incorporates: encrypting means (B3) for producing a customized cipher (C) from the customized data prior to the signature S of the message (m), means (B5) for producing a combination of a message m to be signed and the cipher (C) associated with said message, for example in the form of a concatenation of the message (m) with the cipher (C), and means (B6) for signing (Sig) the message (m) with the customized data (z; K) in the form of a cipher (C) associated with said message. Advantageously, the physical medium is a smart card (26) or the like.

[Suite sur la page suivante]

WO 03/056750 A2

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le système permet à un membre (M) d'un groupe (G) de produire, à l'aide d'une donnée personnalisée (z ; K), un message (m) accompagné d'une signature (S) prouvant à un vérifieur que le message provient d'un membre du groupe (G), et se caractérise par le fait que la donnée personnalisée se présente sous forme intégrée à un support matériel électronique (26). Ce dernier intègre avantageusement aussi : des moyens (B3) de chiffrement pour réaliser un chiffré (C) personnalisé à partir de la donnée personnalisée préalablement à la signature S du message (m), des moyens (B5) pour réaliser une combinaison d'un message m à signer et le chiffré C associé à ce message, par exemple sous forme de concaténation du message m avec le chiffré (C), et des moyens (B6) de signature (Sig) du message (m) avec la donnée personnalisée (z ; K) sous forme de chiffré (C) associé à ce messge. Avantageusement, le support matériel est une carte à puce (26) ou analogue.

SYSTEME CRYPTOGRAPHIQUE DE SIGNATURE DE GROUPE

L'invention concerne le domaine technique de la sécurité des services, et plus précisément de la signature électronique de message, au moyen de la cryptographie.

On rappelle que la signature électronique est un mécanisme relevant de la cryptographie dite à clé publique: le signataire possède une clé secrète et une clé publique associée. Il produit la signature d'un message à l'aide de sa clé secrète. Le vérifieur a uniquement besoin de la clé publique pour vérifier la signature.

Plus précisément encore, l'invention concerne les signatures (électroniques) de groupe. Une signature de groupe permet aux membres d'un groupe de produire une signature telle que le vérifieur reconnaîtra cette signature comme ayant été produite par un membre du groupe, tout en ignorant de quel membre il s'agit. Cependant, une autorité de confiance a la possibilité de lever à tout moment cet anonymat et donc de révéler l'identité du signataire. De telles signatures sont bien souvent "non-corrélables" : il est impossible de déterminer si deux signatures ont été émises par la même personne ou non.

Dans tout schéma classique de signature de groupe, est attribuée au groupe une unique clé publique de groupe, tandis qu'est attribué à chaque membre de ce groupe un identifiant et une clé privée qui leur sont propres. A l'aide de sa clé privée, un membre du groupe peut produire une signature de groupe d'un message de son choix, laquelle signature peut être vérifiée par une entité quelconque à l'aide de la clé publique de groupe. La vérification apprend seulement à cette entité que la signature a été produite par un membre du groupe, mais ne lui donne aucune information sur l'identifiant du membre qui a signé. En revanche, l'autorité de confiance dispose d'une information supplémentaire qui lui permet de retrouver l'identifiant de

ce membre, et donc de lever cet anonymat à tout moment (on dit que l'autorité de confiance "ouvre" la signature).

Les signatures de groupe ont beaucoup d'applications parmi lesquelles les deux suivantes.

Une première application, décrite par référence à la figure 1, est donnée par les enchères électroniques. Elles mettent en place trois protagonistes : un serveur d'enchères 2, une autorité de confiance 4 et un client Cl. L'ensemble des clients forme un groupe G dit "groupe des clients". Un utilisateur désirant s'inscrire au groupe des clients G doit s'adresser à l'autorité de confiance 4, qui lui fournit sa clé privée SK. Il obtient ainsi le droit de produire une signature de groupe. Muni de ce droit, il pourra signer chacune de ses enchères de manière anonyme. Lors d'une enchère pour un certain produit, chaque membre du groupe des clients peut enchérir en signant un message contenant notamment le produit mis en vente et le montant de son enchère. Le serveur d'enchères 2 peut vérifier l'appartenance au groupe et donc la validité de l'enchère simplement en vérifiant la signature de groupe. Le vainqueur est celui qui donne la dernière enchère avant l'adjudication. Le dernier message reçu par le serveur d'enchères est donc celui du vainqueur. Le serveur adresse alors ce message et la signature de groupe correspondante à l'autorité de confiance 4, qui est la seule capable d'en lever l'anonymat et donc de déterminer l'identité physique de l'acheteur du produit mis aux enchères.

Les enchères se doivent d'être rapides. En effet, elles se déroulent pendant un temps très court où parfois le premier qui enchérit à un prix donné a des chances de gagner la partie parce qu'il aura atteint un niveau trop haut pour les autres. C'est pourquoi le mécanisme de signature de son offre ne doit pas prendre trop de temps.

Une seconde application, décrite par référence à la figure 2, est le paiement électronique anonyme. Elle met en

place quatre protagonistes : un client Cl, un commerçant 6, une banque 8 et une autorité de confiance 4. Chaque client Cl doit se faire enregistrer dans le système et obtenir une clé privée SK d'un schéma de signature de groupe avant de pouvoir effectuer sa première transaction. Pour effectuer un paiement, le client doit retirer des pièces électroniques PE auprès de sa banque 8. On rappelle qu'une pièce électronique représente une donnée (un numéro de série) signée numériquement par la banque. Les pièces PE qu'il retire sont anonymes grâce à l'utilisation d'un mécanisme dit de signature aveugle.

La dépense d'une pièce PE chez un commerçant 6 se fait de la manière suivante : le client (Cli dans l'exemple) génère une signature de groupe portant sur la pièce électronique PE et transmet l'ensemble (signature et PE) au commerçant. Si la pièce est valide (vérification de la signature de la banque) et la signature de groupe est authentique, le commerçant accepte la transaction. En fin de journée (ou au moment le plus opportun), le commerçant transmet à la banque les signatures et les pièces reçues en paiement pour compensation de leur valeur. En cas de fraude (réutilisation d'une même pièce dans plusieurs transactions par exemple), la banque 8 envoie la signature de groupe portant sur la pièce litigieuse à l'autorité de confiance 4 afin qu'elle identifie le client indélicat et sanctionne le contrevenant.

Il existe de nombreux articles proposant des schémas de signature de groupe. Actuellement, deux d'entre eux sont les plus souvent cités : i) J. Camenisch, M. Stadler "Efficient group signature scheme for large groups" In B.Kaliski, Advances in Cryptology; Eurocrypt'97, vol.1294 de LNCS, pages 410-424. Springer Verlag, 1997, et ii) G. Ateniese, J. Camenisch, M. Joye, G. Tsudik "A practical and provably secure coalition-resistant group signature scheme"

In M. Bellare Advances in Cryptology - CRYPTO 2000, vol. 1880 de LNCS, pages 225-270. Springer Verlag.

Ils sont tous les deux basés sur la même idée générale qui est la suivante.

Tout d'abord, ils considèrent un schéma de signature ordinaire, par exemple selon l'algorithme RSA (Rivest, Shamir, Adleman), un schéma de chiffrement probabiliste (si on chiffre deux fois le même message, les chiffrés correspondants sont différents) et sémantiquement sûr (il est impossible d'apprendre une quelconque information sur le texte clair à partir du chiffré).

Ensuite, une autorité de confiance 4 responsable du groupe G génère les clés de chiffrement et de signature, puis met les clés publiques correspondantes dans un endroit généralement accessible, par exemple un annuaire. Elle garde secrète les clés privées SK associées.

Pour devenir membre du groupe, une personne détermine un identifiant (valeur numérique que l'autorité de confiance peut relier à la personne physique ou morale membre du groupe) et interagit avec l'autorité de confiance 4 pour obtenir un certificat de membre qui est en fait la signature de l'identifiant à l'aide de la clé privée SK de signature de l'autorité de confiance.

Pour signer un message m au nom du groupe, le membre en question réalise deux actions :

- action i) : chiffrer son identifiant à l'aide de la clé publique de chiffrement de l'autorité de confiance (cette partie servira à ouvrir éventuellement la signature) et

- action ii) : faire la preuve qu'il connaît un certificat de membre associé au texte clair inclus dans le chiffré (preuve qu'il fait bien partie du groupe).

On se base ici sur la cryptographie, et plus particulièrement sur les preuves de connaissance pour

obtenir les propriétés voulues sur les signatures de groupe.

La vérification de la signature consiste à vérifier la preuve de connaissance, par exemple du type à connaissance nulle. L'ouverture de la signature est le simple déchiffrement de l'identifiant.

L'inconvénient majeur d'un tel principe est le poids des calculs. En effet, chaque signature nécessite de réaliser un chiffrement (action i) et surtout un certain nombre de preuves de connaissance (action ii) qui sont en pratique très coûteuses en temps de calcul, puisque mettant en oeuvre de nombreuses exponentiations modulaires (par exemple, il faut environ une seconde par exponentiation modulaire avec une carte à puce munie d'un cryptoprocesseur).

Au vu de ce qui précède, la présente invention a pour but de mettre en place un schéma de signature de groupe qui soit très rapide, c'est-à-dire ne demandant que très peu d'exponentiations modulaires (dans les exemples typiquement une ou deux exponentiations au maximum), tout en gardant les propriétés des schémas de signature de groupe actuels (taille de signature constante, schéma sûr, clé publique inchangée à l'arrivée d'un nouveau membre, etc.).

Sur le plan industriel, elle permet ainsi une mise en œuvre rapide même en utilisant des supports de calcul à capacité réduite, telles que des cartes à puce et dispositifs communicants portatifs analogues.

Plus particulièrement, l'invention prévoit, selon un premier objet, un système de signature de groupe permettant à un membre d'un groupe de produire, à l'aide d'une donnée personnalisée, un message accompagné d'une signature prouvant à un vérifieur que le message provient d'un membre du groupe,

caractérisé en ce que la donnée personnalisée se présente sous forme intégrée à un support matériel électronique.

Dans un mode de réalisation préféré, le support matériel électronique intègre également des moyens de chiffrement pour réaliser un chiffré personnalisé à partir de ladite donnée personnalisée préalablement à la signature du message, des moyens pour réaliser une combinaison d'un message à signer et le chiffré associé à ce message, par exemple sous forme de concaténation du message avec le chiffré, et des moyens de signature du message avec la donnée personnalisée sous forme de chiffré associé à ce message.

La donnée personnalisée peut être un identifiant personnel au membre, le support matériel électronique intègrant en outre une clé de chiffrement commune aux membres du groupe, et les moyens de chiffrement réalisant un chiffré de l'identifiant avec cette clé de chiffrement.

De préférence, les moyens de chiffrement réalisent un chiffré de l'identifiant et d'un aléa.

En variante, la donnée personnalisée peut être une clé de chiffrement diversifiée, propre à chaque membre du groupe, les moyens de chiffrement réalisant un chiffré d'au moins une donnée, par exemple un aléa, avec la clé de chiffrement.

Les moyens de chiffrement peuvent mettre en œuvre un algorithme de chiffrement à clé secrète, par exemple l'algorithme connu par la désignation AES (advanced encryption standard), ou un algorithme de chiffrement à clé publique, par exemple l'algorithme connu par la désignation RSA (Rivest, Shamir, Adleman).

Avantageusement, les moyens de signature mettent en œuvre un algorithme de signature à clé privée, par exemple l'algorithme connu par la désignation RSA, celui-ci pouvant inclure la norme dite PKCS#1 telle que définie notamment

dans le document "RSA Cryptography Standard - RSA Laboratories. Draft2 - 5 janvier 2001".

Avantageusement, le support matériel électronique est un dispositif communicant portatif, notamment une carte à puce.

Selon un deuxième aspect, l'invention concerne également un procédé d'émission d'un message avec une signature de groupe de ce message, caractérisé en ce qu'il met en œuvre le système selon le premier aspect, la signature du message étant produite avec une clé SK privée commune aux membres du groupe et intégrant la donnée personnalisée produite à partir du support matériel électronique,

le procédé prévoyant de transmettre le message ainsi signé à un vérifieur sans recours à une fourniture de preuve à ce dernier de l'appartenance de membre audit groupe, tel qu'un certificat de membre ou la preuve de possession d'un tel certificat.

Selon un troisième aspect, l'invention concerne un procédé de vérification d'un message reçu avec une signature de groupe de ce message, le message ayant été émis conformément au procédé selon le deuxième aspect, caractérisé en ce que la vérification est réalisée au moyen d'une clé publique qui correspond à ladite clé privée.

Selon un quatrième aspect, l'invention concerne un procédé d'ouverture d'une signature produite par le système selon le premier aspect, caractérisé en ce qu'il comprend les étapes consistant à :

- mettre à disposition préalablement à la signature des données de correspondance entre les identités des membres du groupe et leur donnée personnalisée ;
- déchiffrer la donnée personnalisée reçue à partir d'un support matériel électronique dont la signature est à ouvrir ; et

- mettre en correspondance la donnée personnalisée déchiffrée avec l'identité du membre du groupe.

Selon un cinquième aspect, l'invention concerne un procédé de préparation d'un support matériel électronique du système selon le premier aspect, personnalisé à un membre admis à un groupe, caractérisé en ce qu'il comprend les étapes consistant à :

- produire la donnée personnalisée destinée audit support matériel électronique à personnaliser ; et
- inscrire cette donnée personnalisée avec une clé privée de signature dans le support.

L'invention et les avantages qui en découlent apparaîtront plus clairement à la lecture de la description qui suit des modes de réalisation préférés, donnés purement à titre d'exemples non-limitatifs, par référence aux dessins annexés dans lesquels :

- la figure 1, déjà décrite, est un schéma de principe illustrant un exemple de codage de groupe dans le cadre d'une vente aux enchères ;
- la figure 2, déjà décrite, est un schéma de principe illustrant un exemple de codage de groupe dans le cadre d'achats par des pièces électroniques ;
- la figure 3 est un schéma servant à illustrer des transactions au moyen d'une carte à puce pour la signature de messages conformément à l'invention ;
- la figure 4 est un schéma bloc des éléments fonctionnels d'une carte à puce pouvant être utilisée pour réaliser les signatures de groupe conformément à l'invention ;
- la figure 5 est un organigramme général des éléments fonctionnels qui interviennent au sein d'une carte à puce pour réaliser les signatures de groupe conformément à l'invention ;

- la figure 6 est un organigramme d'un premier exemple de mise en œuvre d'éléments spécifiques vis-à-vis de l'organigramme de la figure 5 ;

- la figure 7 est un organigramme selon une variante du premier exemple, et

- la figure 8 est un organigramme d'un deuxième exemple de mise en œuvre d'éléments spécifiques vis-à-vis de l'organigramme de la figure 5.

Conformément à l'invention, plutôt que d'envisager les deux actions i) et ii) précitées de l'état de la technique, on prévoit une approche selon laquelle l'identifiant n'est plus associée directement à une personne physique ou morale, mais intégré à un dispositif électronique communicant attribué à un membre autorisé d'un groupe. Dans le mode de réalisation, le dispositif, qui est typiquement portatif tel qu'une carte à puce ou un boîtier incorporant celle-ci (par exemple un terminal de téléphone mobile), comprend avantageusement sur un même ensemble physique : une donnée personnalisée (identifiant ou clé de chiffrement diversifiée) mémorisée sous forme électronique, les moyens pour chiffrer cette donnée, et les moyens pour réaliser la signature de groupe sur l'ensemble comprenant le message à transmettre et le chiffré de la donnée personnalisée.

Un exemple de mise en œuvre de l'invention est représenté à la figure 3 pour le cas d'un membre M d'un groupe G qui réalise, à l'aide d'une carte à puce personnalisée 26, des transactions avec des prestataires de service, en l'occurrence un serveur d'enchères 2 et un commerçant 6. La communication entre un membre M et un prestataire peut se faire par tout moyen connu, par exemple depuis son ordinateur personnel (PC) 10 via un réseau de communication, tel qu'Internet, ou par un téléphone mobile 27 équipé d'un lecteur 27a de carte à puce externe, l'échange de données avec les prestataires de service 2, 6

s'effectuant alors par voie hertzienne 29 via l'antenne 27b du téléphone mobile.

L'ordinateur personnel 10 comprend notamment une unité centrale 14, une carte modem 16 ou autre interface de communication avec le réseau 12, un écran de visualisation 18, et un clavier 20 avec dispositif de pointage 22. Il comprend également un lecteur de carte à puce 24 par laquelle la carte à puce 26 peut communiquer avec son unité centrale 14 et sur le réseau 12. La partie puce 26a de la carte est de préférence du type sécurisé.

Les services offerts par le serveur d'enchères 2 et le commerçant 6 sont identiques à ceux décrits dans le cadre respectivement des figures 1 et 2, et ne seront pas décrits à nouveau par souci de concision. De même, leur mode de fonctionnement avec la banque 8 (pour le commerçant 6) et l'autorité de confiance 4 est sensiblement le même.

Conformément à l'invention, l'autorité de confiance 4 délivre un identifiant z à un membre M accepté par elle du groupe G directement sous forme matérielle, en l'occurrence sous forme de la carte à puce personnalisée 26 avec une puce sécurisée 26a.

L'inscription de la donnée personnalisée dans une carte (sous forme d'identifiant z ou de clé K diversifiée désignée Kz) s'effectue par un protocole d'échange de données via une borne gérée par l'autorité de confiance. La donnée personnalisée est établie et stockée au sein de la carte durant cet échange.

L'autorité de confiance 4 peut également établir la donnée personnalisée avec une carte à puce existante dès lors que cette carte soit à même de permettre le chargement de données après qu'elle soit émise. Ceci est notamment le cas avec des cartes polyvalentes destinées à intégrer de nouvelles applications à tout moment par chargement à partir d'une borne, permettant de réunir plusieurs services ou fonctions distincts sur un seul support.

L'autorité de confiance associe donc un membre (personne physique ou morale, désigné de manière générique par le terme "personne") du groupe G à sa donnée personnalisée par le biais de la carte personnalisée 26 émise pour cette personne. Celle-ci n'aura donc pas de lui-même à enregistrer sa donnée personnalisée et à fournir la preuve cryptographique qu'il la possède.

Une carte personnalisé 26 est émise à une personne candidate par l'autorité de confiance 4 lorsque cette personne remplie les conditions pour devenir membre du groupe G, avec les vérifications et précautions d'usage, à l'instar de l'émission d'une carte bancaire classique. L'autorité de confiance enregistre notamment la correspondance entre la donnée personnalisée contenue dans une carte 26 émise et l'identité (par exemple le nom) de la personne à qui cette carte à été rendue.

En résultat, la sécurité repose ici d'une part, sur un dispositif contenant une puce sécurisée 26a et, d'autre part, sur une clé. Celle-ci peut être soit partagée par tous les membres M du groupe G pour générer une signature de groupe lorsque la donnée personnalisée est un identifiant à chiffrer par cette clé, soit diversifiée, c'est-à-dire spécifique au membre lorsqu'elle constitue elle-même la donnée personnalisée. Les aspects détaillés de cette approche sont présentés dans ce qui suit.

Tout d'abord, les modes de réalisation de l'invention font appel à un schéma de signature ordinaire S et un algorithme de chiffrement probabiliste et sémantiquement sûr (algorithme à clé publique ou à clé secrète). Ensuite, l'autorité de confiance 4 responsable du groupe génère la ou les clé(s) de signature SK ou analogue, puis met dans un annuaire la clé publique correspondante. Elle garde secrète la clé privée de signature, puis elle publie toutes les informations nécessaires à la mise en oeuvre de l'algorithme de chiffrement.

Pour devenir un membre, une personne obtient auprès de l'autorité de confiance 4 une carte à puce 26 contenant d'une part, soit un identifiant z,soit une clé K diversifiée (l'autorité de confiance gardant en mémoire le lien entre la carte à puce, l'identifiant z, et le clé K diversifiée ainsi que le nouveau membre M), et d'autre part, la clé privée de signature SK. Celle-ci est donc en fait une clé partagée entre tous les membres du groupe G. La carte possède de plus toutes les informations nécessaires au chiffrement à l'aide de l'algorithme fourni par l'autorité de confiance. Muni de cet ensemble d'éléments intégrés dans la carte à puce 26, le membre M peut, à l'aide de cette dernière, signer un message m au nom du groupe G, cette signature S pouvant être ouverte par l'autorité de confiance (et par elle seule) si cela est nécessaire.

Pour signer un message m au nom du groupe, le membre utilise sa carte à puce qui va prendre en entrée le message m. La carte va dans un premier temps réaliser un chiffrement spécifique au membre à l'aide de l'algorithme de chiffrement de l'autorité de confiance, puis signer le message constitué de au moins le message m de départ et le chiffré obtenu précédemment, cette signature étant produite à l'aide de la clé privée partagée de signature qu'elle possède en mémoire. En sortie, la carte à puce 26 envoie au destinataire 2, 6 (vérifieur) le message, le chiffré et la signature.

La vérification de la signature consiste simplement à vérifier la signature générée par la clé privée partagée, à l'aide de la clé publique correspondante. L'ouverture de la signature par l'autorité de confiance 4 consiste à déchiffrer la donnée personnalisée et à trouver la correspondance avec l'identité du possesseur de la carte à puce 26.

Le résultat est très rapide au niveau de la carte, puisque au moment de la signature S il n'y a qu'un chiffrement et une signature à effectuer (et donc au maximum deux exponentiations modulaires).

Contrairement à l'état de l'art relatif aux signatures de groupe où le lien entre l'identifiant et le message est réalisé par des mécanismes cryptographiques (preuves de connaissance), l'invention utilise une approche matérielle avec une sécurité reposant sur celle d'un objet, avantageusement sécurisé, en l'occurrence la carte à puce 26.

Le principe de fonctionnement des modes de réalisation au niveau de la carte à puce est décrit de manière plus détaillée par référence aux organigrammes des figures 5 à 7. Au préalable, l'architecture général d'une carte à puce pouvant être utilisée dans le cadre de l'invention est décrite par référence à la figure 4.

La figure 4 représente sous forme de schéma bloc simplifié les éléments fonctionnels selon une architecture possible de la carte à puce 26. Ces éléments comprennent :

- un microprocesseur 28 assurant la gestion de fonctions internes et l'exécution de programmes applicatifs de la carte. Il peut comprendre notamment un "cryptoprocesseur" optimisé pour les calculs crytographiques ;

- une mémoire vive accessible en écriture 30 (désignée RAM de l'acronyme anglo-saxon "random access memory"). Cette mémoire sert entre autres à l'enregistrement de données éphémères, par exemple les résultats intermédiaires de calculs algorithmiques ;

- une mémoire rémanente 32 de technologie programmable et à effacement électronique (désignée EEPROM de l'acronyme anglo-saxon "electrically erasable programmable read-only memory (ROM)). Cette mémoire sert notamment pour le stockage de données à long terme après la

fabrication de la carte, par exemple la donnée personnalisée de la carte, le code logiciel lié aux algorithmes utilisés, etc. ;

- une mémoire figée 34 du type ROM "masque", programmée avec des données immuables lors de son procédé de fabrication à l'aide de masques. Cette mémoire enregistre notamment le code de gestion interne de la carte, mais peut également stocker des données du cryptage communes aux membres du groupe. Le partage du stockage des données entre les mémoires EEPROM 32 et ROM masque 34 est au choix du concepteur ;

- une interface de communication 36 par laquelle la carte échange des données avec l'environnement extérieur, tel que le lecteur de carte 24 ou 27a ; et

- un bus interne 38 qui relie les éléments précités.

Le principe général du fonctionnement de la carte 26 pour la signature de messages est représenté à la figure 5. Cette figure comporte un cadre à l'intérieur duquel tous les éléments - données ou actions - se situent au sein même de la carte à puce, d'où sa désignation 26. Dans le cas illustré, la donnée personnalisée est sous la forme d'un identifiant z.

Pour chaque message m à transmettre devant porter la signature S du groupe, la carte 26 soumet son propre identifiant z (case B1) à un algorithme de chiffrement (désignation générique E) (case B2). La case B1 est représentée en pointillés, s'agissant d'un élément qui peut être supprimé en cas d'utilisation d'une clé diversifiée Kz. Concrètement, cette action consiste à faire exécuter par le microprocesseur 28 le code de l'algorithme E lu à partir de l'EEPROM 32 et, le cas échéant, de la mémoire ROM masque 34, avec insertion, en tant que paramètre, de l'identifiant z lu en interne à partir d'une mémoire de la carte, par exemple la mémoire EEPROM 32. L'algorithme E

fait également intervenir au moins un autre paramètre, tel qu'un nombre aléatoire et une clé de chiffrement, comme décrit plus loin par référence aux exemples. Le résultat de l'algorithme E sur l'identifiant z est le chiffré de l'identifiant, désigné C = E(z) (case B3). Le chiffré C et ensuite stocké provisoirement en interne dans la mémoire RAM 32.

En parallèle, la carte réceptionne le message m à signer sur son interface de communication 36 et l'enregistre provisoirement dans la mémoire RAM 32 (case B4).

Ensuite, la carte réalise la concaténation m' du message m et du chiffré C (case B5), soit m' = m||C. Cette opération consiste à produire un séquence binaire comportant la suite des bits du message m suivie/précédée des bits du chiffré C.

La concaténation m' est ensuite fournie en tant que paramètre à un autre algorithme, dit de signature (désignation générique Sig) (case B6), qui produit la signature de m' à l'aide d'une clé privée de signature SK. Concrètement, cette opération consiste à faire exécuter par le microprocesseur 28 le code de l'algorithme Sig lu à partir de l'EEPROM 32 et, le cas échéant, de la ROM masque 34, avec insertion, en tant que paramètre, d'une part la clé de signature SK, lue en interne à partir d'une mémoire de la carte, par exemple la mémoire EEPROM 32, et d'autre part la concaténation m' lue à partir de la mémoire RAM 30.

La signature authentifiée S du message m ainsi produite par cet algorithme Sig est alors transmise en sortie à l'interface de communication 36 de la carte 26 pour exploitation dans le cadre du système de transaction de groupe G. Plus particulièrement, le signature produite avec la clé privée de signature SK sur l'opérande m', soit $Sig_{SK}(m')$, forme un ensemble transmis depuis l'ordinateur

personnel 10 ou le téléphone mobile 27 vers un prestataire de services 2 ou 6.

Ces derniers, agissant en tant que "vérifieur", peuvent établir si le message m extrait de la signature $Sig_{SK}(m')$ provient effectivement d'une carte authentique 26 au moyen d'un algorithme de vérification (désignation générique $Ver_{PK}(m',S)$) et d'une clé publique PK mise à la disposition générale par l'autorité de confiance 4. Cet algorithme est de nature dichotomique, produisant une réponse oui/non.

Au niveau de l'autorité de confiance 4, la signature est ouverte au moyen d'un algorithme de déchiffrement D permettant de retrouver la correspondance entre l'identifiant z et l'identité du possesseur de la carte à puce 26, soit z = D(C).

Le tableau I résume les entités utilisés par les différents protagonistes dans ce cadre général :

Tableau I : liste des entités utilisées par un membre M(carte 26), un vérifieur V et l'autorité de confiance pour le mode de réalisation général.

Eléments utilisés par Membre M (carte 26)	**Eléments utilisés par Vérifieur V (prestataire de services 2, 6)**
message m	clé publique PK
identifiant z	$Ver_{PK}(m',S)$ = oui/non
clé privée SK	
C = E(z)	
m' = m||C	
$S = Sig_{SK}(m')$	
Eléments utilisés par l'autorité de confiance 4	
z = D(C)	

Il sera maintenant décrit deux exemples particuliers basés sur le mode de réalisation général de la figure 5,

par référence respectivement aux figures 6 à 8. Chacune de ces figures est un organigramme basé sur celui de la figure 5. Les éléments (cases) des figures 6 à 8 qui correspondent à ceux de la figure 5, mais sous forme spécifique, portent les mêmes références suivi d'un signe "'" (prime) pour le cas de la figure 6 et d'un signe "''" (double prime) pour le cas de la figure 7 ; les éléments identiques entre les figures 5 et les figures 6 à 8 portent les mêmes références. Les aspects communs aux figures 6 à 8 déjà décrites par référence à la figure 5 ne seront pas répétés par souci de concision.

Exemple 1 : mode de réalisation basé sur l'algorithme de chiffrement AES et de signature RSA

Dans cet exemple (figure 6), le schéma de signature choisi est l'algorithme RSA. Le module sera noté n, la clé privée est SK et correspond à la clé partagée ; la clé publique est PK. L'algorithme de chiffrement choisi dans l'exemple est AES (de l'anglais "advanced encryption standard") qui est donc un algorithme à clé secrète. On note K la clé associée. Dans ce cas illustré, il s'agit d'un clé partagée parmi tous les membres M du groupe G. L'autorité de confiance publie PK et garde toutes les autres clés secrètes.

Conformément à ce premier exemple, l'algorithme AES de chiffrement B2' accepte en tant que paramètre d'entrée : i) l'identifiant z (case B1), ii) une clé secrète de chiffrement K (case B8) partagée parmi tous les membres M admis au groupe G et stockée dans la mémoire EEPROM 32 et iii) un aléa r (case B9). Ce dernier est un nombre aléatoire d'une longueur binaire prédéterminée, générée au sein de la carte 26 au moyen d'un code logiciel exécuté par le microprocesseur 28. L'aléa r est renouvelé à chaque signature de message m.

L'algorithme AES produit alors le chiffré C de l'identifiant et de l'aléa r avec AES et la clé secrète K (case B3').

Ce chiffré C est ensuite soumis à une concaténation m' = m||C (case B5), puis fourni en tant que paramètre d'entrée à un algorithme de signature de type RSA (Rivest, Shamir, Adleman) (case B6'). Cet algorithme prend en entrée une clé privée de signature SK (case B7), avec lequel il produit la signature RSA de m", soit $S = m"^{SK} \bmod n$, où m" = le résultat de PKCS#1 sur m'; où "mod n" signifie l'arithmétique modulo n et PKCS#1 est une norme définie notamment dans le document "RSA Cryptography Standard – RSA Laboratories. Draft2 – 5 janvier 2001".

Le tableau II résume les entités utilisées par les différents protagonistes du groupe G selon le premier exemple:

Tableau II : liste des éléments utilisés par un membre M(carte 26), un vérifieur V et l'autorité de confiance selon l'exemple 1.

Eléments utilisés par Membre M (carte 26)	**Eléments utilisés par Vérifieur V (prestataire de services 2, 6)**
message m	clé publique PK
identifiant z	$m" = S^{PK} \bmod n$?
clé privée SK	
aléa r	
C = AES(z,K,r)	
m' = m||C	
m" = PKCS#1(m')	
$S = m"^{SK} \bmod n$	
Eléments utilisés par l'autorité de confiance 4	
z = AES(C,K)	
z ⇔ M	

Une sécurité supplémentaire consiste à scinder l'autorité de confiance en deux. La première possède uniquement la clé privée SK (et n'a pas connaissance des identifiants des membres) : c'est l'autorité de groupe (c'est elle qui intervient lors de la phase d'inscription au groupe). La seconde possède seulement la clé K ainsi que tous les identifiants des membres du groupe : c'est l'autorité d'ouverture (c'est elle qui intervient lors de la phase d'ouverture des signatures). Ainsi, une autorité, seule, ne peut pas se faire passer pour l'un des membres. Cette approche ressort du principe qu'il est préférable de ne pas confier toute la sécurité du système à une seule autorité.

A l'arrivée d'un nouveau membre dans le groupe, l'autorité de confiance crée pour lui une nouvelle carte à puce et place dans sa mémoire n, SK et K ainsi qu'une valeur z (l'identifiant du membre). Elle note dans sa base de donnée que la valeur z est associée à ce nouveau membre.

Lorsque ce membre désire signer un message, il insère sa carte dans un lecteur et lui demande de signer le message m. Dans un premier temps, la carte à puce utilise l'algorithme AES avec comme entrées la clé K, la valeur z et un aléa r (le chiffrement est ainsi probabiliste) pour obtenir en sortie le chiffré C.. Ensuite, elle fabrique le message m' en concaténant le message m et le chiffré C qu'elle vient d'obtenir, puis modifie le résultat en un message m" selon par exemple la norme PKCS#1. Enfin, elle calcule $S = m"^{SK}$ modn. Le couple (S, C) est la signature de groupe du message m.

Le vérifieur n'a besoin que de n et de PK pour vérifier que la signature vient bien d'un membre du groupe. Il n'a qu'à vérifier que $m"= S^{PK}$ modn, conformément à la norme définie plus haut. De plus, ne pouvant déchiffrer C (il ne possède pas la clé K), il n'a aucun moyen de savoir à quel membre il a affaire.

Si l'autorité de confiance désire ouvrir la signature, elle n'aura qu'à utiliser l'algorithme AES et la clé K (il n'a pas besoin de l'aléa r pour déchiffrer) pour obtenir z et regarder dans sa base de données qui correspond à z.

Une variante élevant le niveau de sécurité consiste à choisir la clé Kz de chiffrement diversifiée selon l'identifiant, et de ne chiffrer que l'aléa r, c'est-à-dire d'attribuer une clé Kz différente pour chaque membre M du groupe G.

Dans cette variante, illustrée à la figure 7, on s'affranchit de l'identifiant z en tant que tel, celui-ci n'étant plus nécessaire pour individualiser la carte 26 : l'individualisation est obtenue à la place directement par la clé de chiffrement diversifiée Kz (case B8) du fait qu'elle est individuelle.

Sur le plan matériel, cette variante est mise en œuvre de manière analogue au premier exemple, mais en introduisant comme paramètre dans l'algorithme de chiffrement (celui-ci pouvant toujours être l'algorithme AES) seulement l'aléa r, chargé comme décrit précédemment (case B9), la case B1 étant naturellement supprimée. Le chiffré C qui en résulte est traité de la même manière (case B3' et suivantes). On note que l'aléa r intégré dans le chiffré assure la même fonction de décorréler le message m de sa signature.

Ainsi, si une carte à puce est corrompue, le fraudeur n'aura accès qu'à la clé diversifiée Kz de cette carte, et ne pourra donc pas produire une signature de groupe au nom d'un autre identifiant que celui contenu dans cette carte. La phase d'ouverture consiste alors à tester toutes les clés de chiffrement existantes jusqu'à tomber sur la bonne.

Exemple 2 : mode de réalisation basé sur l'algorithme de chiffrement RSA et de signature RSA

Cet exemple (figure 8) est voisin de celui du premier exemple(figure 6 ou 7), et seulement des différences vis-à-vis de celui-ci seront décrites.

Le schéma de signature choisi est une nouvelle fois l'algorithme RSA. Le module sera noté n, la clé secrète est SK et correspond à la clé partagée ; la clé publique est PK. L'algorithme de chiffrement est cette fois-ci asymétrique puisqu'il s'agit du cryptosystème RSA comme décrit dans la norme précitée. Le module sera noté n'. La clé publique de chiffrement est e et la clé privée associée est d.

A l'arrivée d'un nouveau membre M dans le groupe G, l'autorité de confiance produit une nouvelle carte à puce 26 ou charge des données dans une carte existante et place en mémoire n, n', e et SK, ainsi qu'une valeur z (l'identifiant du membre). Elle note dans sa base de données que la valeur z est associée à ce nouveau membre.

Lorsque ce membre désire signer un message, il insère sa carte 26 dans un lecteur 24 ou 27a et lui demande de signer le message m. Dans un premier temps, la carte va chiffrer son identifiant z à l'aide du cryptosystème RSA (case B2"). Pour cela, elle modifie la valeur z selon par exemple la norme précitée pour obtenir la valeur z' (cette modification prend en paramètre entrée z et un aléa r(case B9)). Elle génère ensuite $C = z'^{e} \bmod n'$, qui est le chiffré de l'identifiant, sur la base de la clé publique e (case B11). Ensuite, elle fabrique le message m' en concaténant le message m et C qu'elle vient d'obtenir (case B5), puis modifie le résultat en un message m" selon par exemple la norme PKCS#1 précitée. Enfin, elle calcule $S = m''^{SK} \bmod n$ (case B6'') sur la base de la clé privée de signature SK. Le couple (S,C) est la signature de groupe du message m.

Le tableau III résume les entités utilisées par les différents protagonistes du groupe G selon le premier exemple:

Tableau III : liste des éléments utilisés par un membre M(carte 26), un vérifieur V et l'autorité de confiance selon l'exemple 2.

Eléments utilisés par Membre M (carte 26)	**Eléments utilisés par Vérifieur V (prestataire de services 2, 6)**
message m	clé publique PK
identifiant z	m" = S^{PK} mod n ?
clé privée SK	
aléa r	
z,r => z'(cf. PKCS#1)	
C = z'^{e} mod n'	
m' = m‖C	
m' => m"(cf. PKCS#1)	
S = $m"^{SK}$ mod n	
Eléments utilisés par l'autorité de confiance 4	
z = C^{d} mod n'	
z' => z (cf. PKCS#1)	
z ⇔ M	

Le vérifieur 2,6 n'a besoin que de la valeur n et de PK pour vérifier que la signature vient bien d'un membre du groupe. Il n'a qu'à vérifier que m" = S^{PK} mod n (cf. la norme PKCS#1 précitée). De plus, ne pouvant déchiffrer C (il ne possède pas la clé K), il n'a aucun moyen de savoir à quel membre il a affaire.

Si l'autorité de confiance 4 désire ouvrir la signature, elle calcule C^{d} mod p pour retomber sur z', puis sur z (la transformation entre z et z' ne nécessite pas la connaissance de l'aléa r et est entièrement décrite par la norme précitée.

Bien entendu, le deuxième exemple permet aussi de scinder l'autorité en deux, comme décrit dans le cadre du premier exemple. De même, il est également envisageable dans ce deuxième exemple d'utiliser comme donnée personnalisée un clé diversifiée, et de s'affranchir de l'identifiant z, à l'instar de la variante de l'exemple 1 (cf. figure 7).

On comprendra de ce qui précède que l'invention présente un avantage remarquable en termes de coûts de calcul, puisqu'il suffit d'avoir au niveau de la carte 26 juste un algorithme de chiffrement et un algorithme de signature, qui ensemble ne nécessitent que deux exponentiations modulaires.

L'invention permet de nombreuses variantes aussi bien au niveau des moyens matériels, cryptographiques, logiciels, communication entre les intervenants, qu'au niveau de applications.

En effet, la signature de messages peut être effectuée par tout dispositif adapté ne relevant pas forcément de la technologie des cartes à puce, tels que objets portatifs spécifiques, assistants personnels communicant, ressources d'un téléphone mobile, etc.

On peut par ailleurs aussi envisager d'autres systèmes algorithmiques que ceux (AES et RSA) des exemples.

La communication entre un membre M et un prestataire peut aussi s'effectuer par des liaisons locales, câblées, hertzien, infrarouge ou autre.

Enfin, les applications données (commerce avec pièces électroniques, ventes au enchères) ne sont que des exemples parmi de nombreuses autres applications possibles.

REVENDICATIONS

1. Système de signature de groupe permettant à un membre (M) d'un groupe (G) de produire, à l'aide d'une donnée personnalisée (z; Kz), un message (m) accompagné d'une signature (S) prouvant à un vérifieur (2, 4) que ledit message provient d'un membre du groupe (G),

caractérisé en ce que ladite donnée personnalisée se présente sous forme intégrée à un support matériel électronique (26).

2. Système selon la revendication 1, caractérisé en ce ledit support matériel électronique (26) intègre des moyens (B3) de chiffrement pour réaliser un chiffré (C) personnalisé à partir de ladite donnée personnalisée (z; Kz) préalablement à la signature S du message (m).

3. Système selon la revendication 2, caractérisé en ce que ledit support matériel électronique (26) intègre en outre des moyens (B5) pour réaliser une combinaison d'un message (m) à signer et le chiffré C associé à ce message, sous forme de concaténation du message m avec le chiffré (C).

4. Système selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit support matériel (26) intègre en outre des moyens (B6) de signature (Sig) du message (m) avec la donnée personnalisée (z; K) sous forme de chiffré (C) associé à ce message.

5. Système selon l'une quelconque des revendications 2 à 4, caractérisé en ce que ladite donnée personnalisée est un identifiant (z) personnel au membre (M) et en ce que ledit support matériel électronique (26) intègre en outre

une clé de chiffrement (K) commune aux membres du groupe (G), les moyens (B3) de chiffrement réalisant un chiffré (C) de l'identifiant avec ladite clé de chiffrement.

6. Système selon la revendication 5, caractérisé en ce que les moyens (B3) de chiffrement réalisent un chiffré (C) de l'identifiant et d'un aléa (r).

7. Système selon l'une quelconque des revendications 2 à 4, caractérisé en ce que ladite donnée personnalisée est une clé de chiffrement (Kz) diversifiée, propre à chaque membre (M) du groupe (G) et en ce que les moyens (B3) de chiffrement réalisent un chiffré (C) d'au moins une donnée (r) avec ladite clé de chiffrement.

8. Système selon la revendication 7, caractérisé en ce que ladite donnée comprend un aléa (r).

9. Système selon l'une quelconque des revendications 2 à 8, caractérisé en ce que les moyens de chiffrement (B3) mettent en œuvre un algorithme de chiffrement à clé secrète (K), par exemple l'algorithme connu par la désignation AES (advanced encryption standard).

10. Système selon l'une quelconque des revendications 2 à 8, caractérisé en ce que les moyens de chiffrement (B3) mettent en œuvre un algorithme de chiffrement à clé publique (e), par exemple l'algorithme connu par la désignation RSA (Rivest, Shamir, Adleman).

11. Système selon l'une quelconque des revendications 4 à 10, caractérisé en ce que les moyens (B6) de signature (Sig) mettent en œuvre un algorithme de signature à clé privée (SK), par exemple l'algorithme connu par la désignation RSA (Rivest, Shamir, Adleman).

12. Système selon la revendication 11, caractérisé en ce que l'algorithme de signature est du type RSA et inclut la norme dite PKCS#1 telle que définie notamment dans le document "RSA Cryptography Standard - RSA Laboratories. Draft2 - 5 janvier 2001".

13. Système selon l'une quelconque des revendications 1 à 12, caractérisé en ce que ledit support matériel électronique est un dispositif communicant portatif (26).

14. Système selon la revendication 13, caractérisé en ce que ledit support matériel électronique est une carte à puce (26).

15. Procédé d'émission d'un message (m) avec une signature (S) de groupe (G) de ce message, caractérisé en ce qu'il met en œuvre le système selon l'une quelconque des revendications 1 à 14, la signature du message (m) étant produite avec une clé (SK) privée commune aux membres (M) du groupe (G) et intégrant la donnée personnalisée (z; Kz) produite à partir du support matériel électronique (26), le procédé prévoyant de transmettre le message ainsi signé à un vérifieur (2, 6) sans recours à une fourniture de preuve à ce dernier de l'appartenance de membre (M) audit groupe (G), tel qu'un certificat de membre ou la preuve de possession d'un tel certificat.

16. Procédé de vérification d'un message (m) reçu avec une signature de groupe de ce message, le message ayant été émis conformément à la revendication 15, caractérisé en ce que ladite vérification est réalisée au moyen d'une clé publique qui correspondant à ladite clé privée (SK).

17. Procédé d'ouverture d'une signature (S) produite par le système selon l'une quelconque des revendications 1 à 14, caractérisé en ce qu'il comprend les étapes consistant à :

- mettre à disposition, préalablement à la signature, des données de correspondance entre les identités des membres (M) du groupe (G) et les données personnalisées ;
- déchiffrer la donnée personnalisée reçue à partir d'un support matériel électronique (26) dont la signature est à ouvrir ; et
- mettre en correspondance la donnée personnalisée déchiffrée avec l'identité du membre (M) du groupe (G).

18. Procédé de préparation d'un support matériel électronique (26) du système selon l'une quelconque des revendications 1 à 14, personnalisé à un membre (M) admis à un groupe, caractérisé en ce qu'il comprend les étapes consistant à :

- produire la donnée personnalisée (z; Kz) destinée audit support matériel électronique (26) à personnaliser ; et
- inscrire cette donnée personnalisée avec une clé privée de signature (SK) dans ledit support.

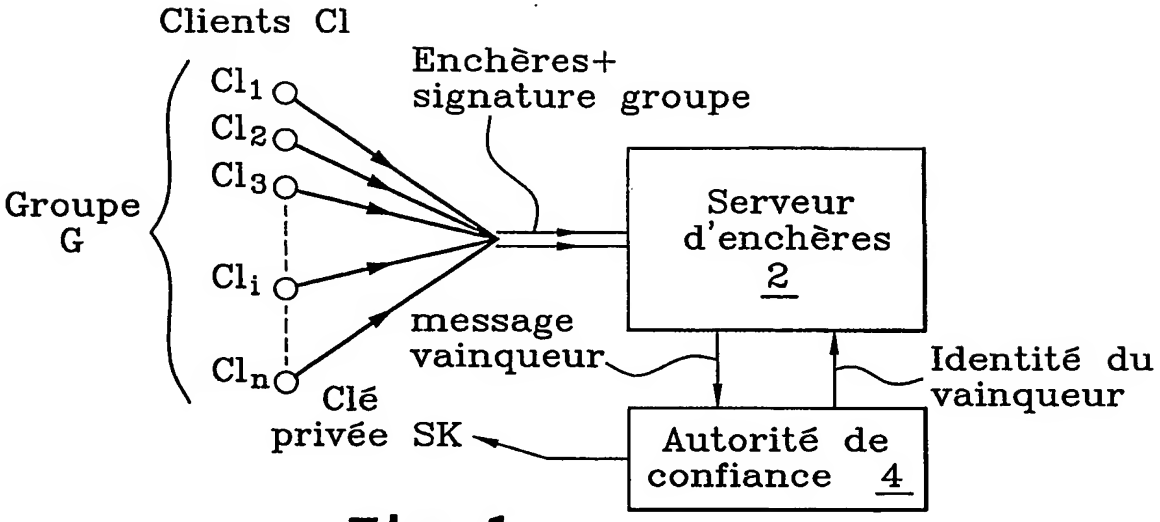

Clients Cl
Groupe G
Cl1
Cl2
Cl3
Cli
Cln
Enchères+ signature groupe
Serveur d'enchères 2
message vainqueur
Identité du vainqueur
Clé privée SK
Autorité de confiance 4

Fig. 1

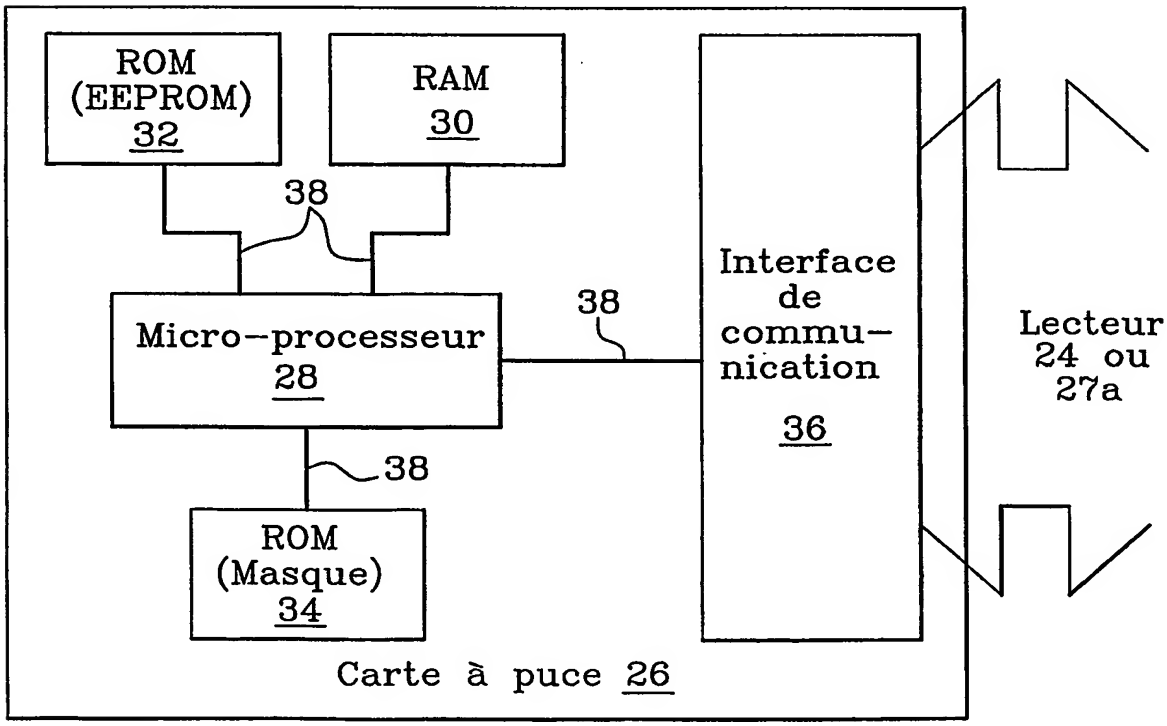

ROM (EEPROM) 32
RAM 30
38
Micro-processeur 28
38
Interface de commu-nication 36
Lecteur 24 ou 27a
38
ROM (Masque) 34
Carte à puce 26

Fig. 4

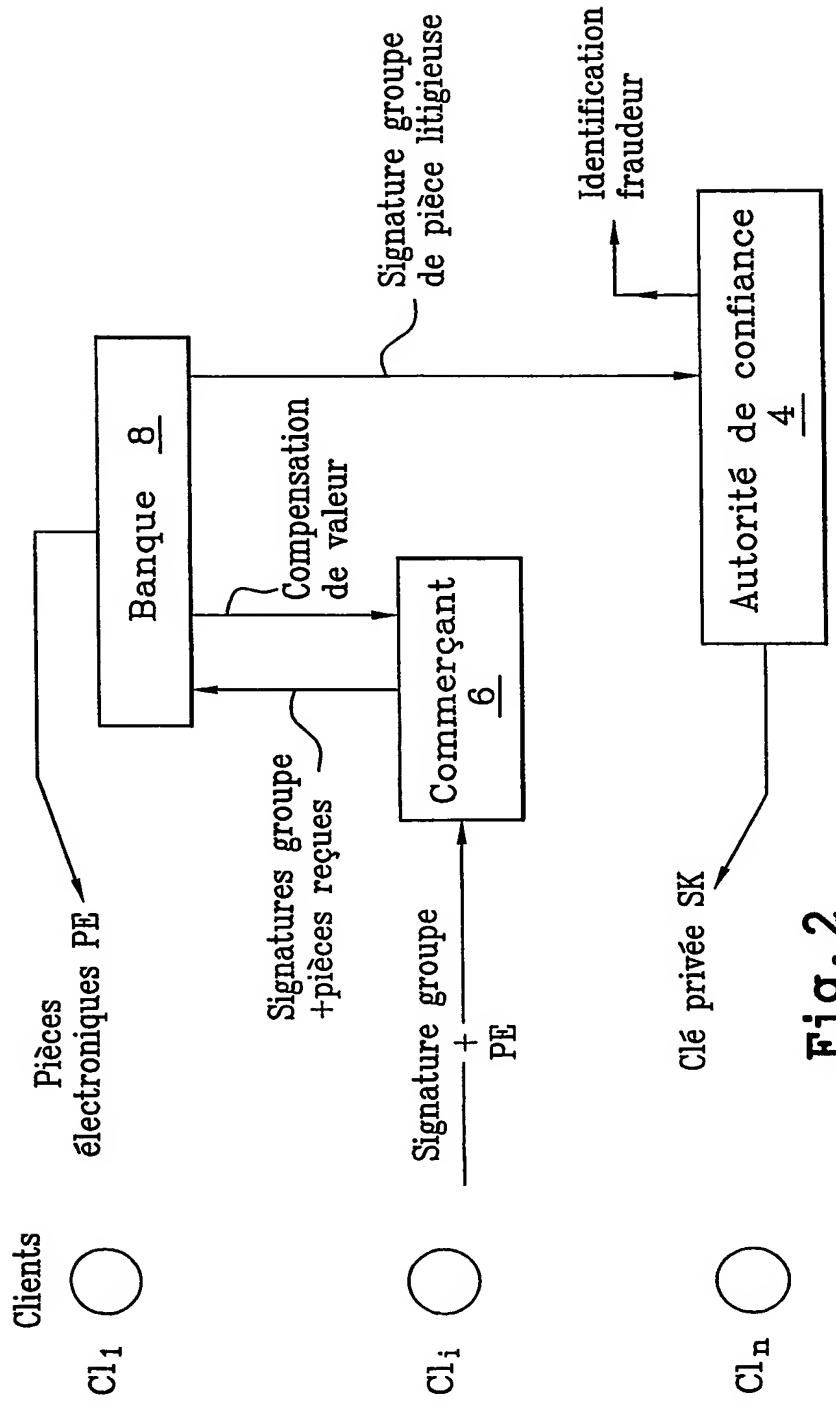

Clients
Cl1
Cli
Cln
Pièces électroniques PE
Banque 8
Compensation de valeur
Signatures groupe +pièces reçues
Signature groupe de pièce litigieuse
Identification fraudeur
Commerçant 6
Signature groupe + PE
Autorité de confiance 4
Clé privée SK

Fig. 2

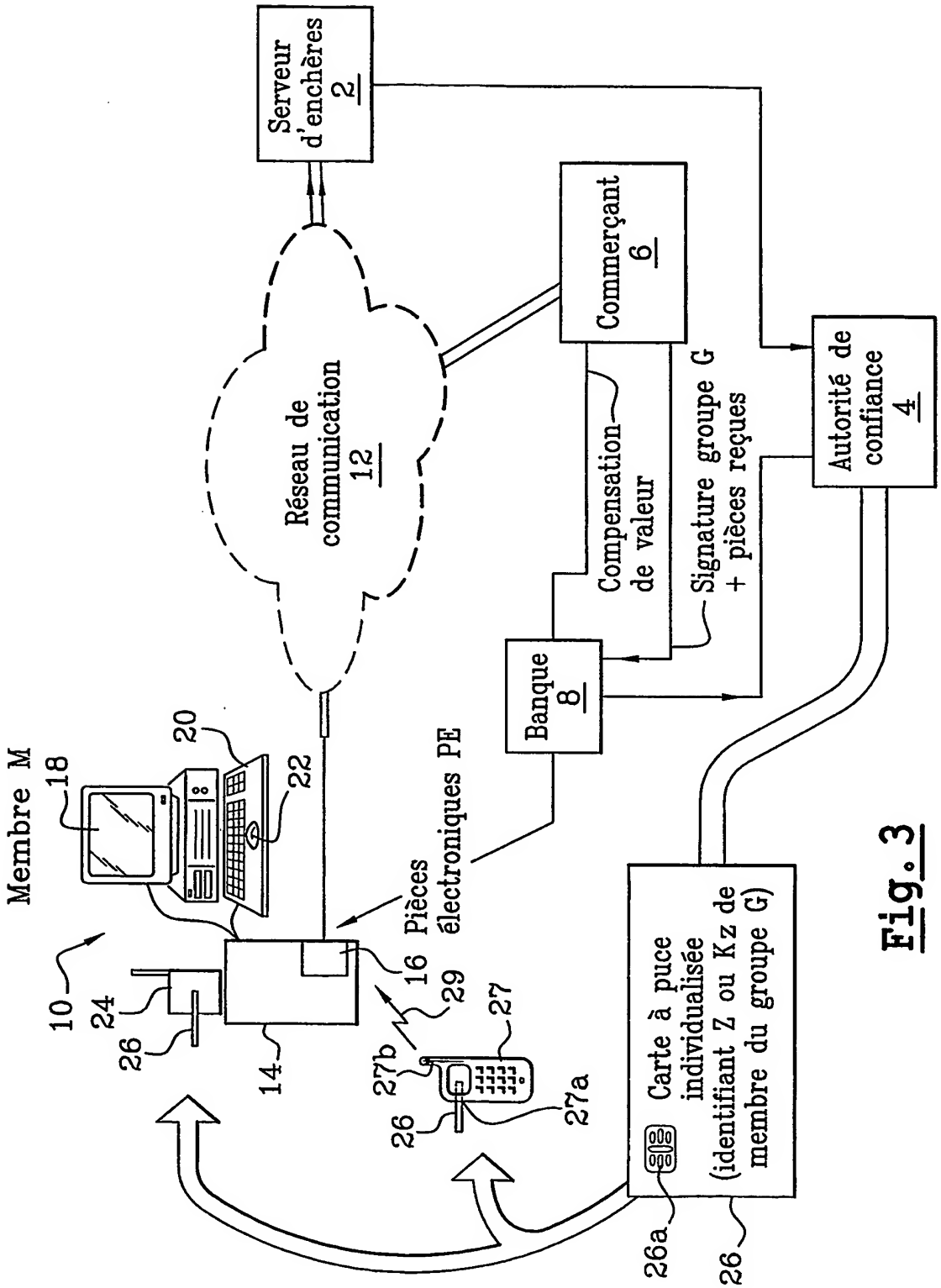

Serveur d'enchères 2
Commerçant 6
Réseau de communication 12
Autorité de confiance 4
Compensation de valeur
Signature groupe G + pièces reçues
Banque 8
Membre M
18
20
22
Pièces électroniques PE
10
24
26
14
16
29
27
27b
27a
Carte à puce individualisée (identifiant Z ou Kz de membre du groupe G)
26a
26

Fig. 3

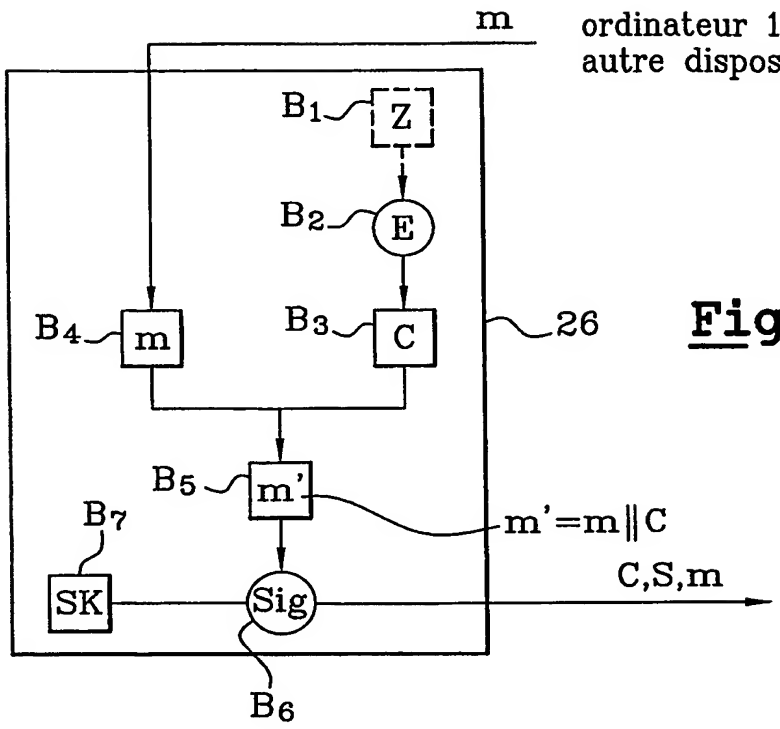

m
ordinateur 10 ou
autre dispositif d'entrée
B1
Z
B2
E
B4
m
B3
C
26
B5
m'
m'=m||C
B7
SK
Sig
C,S,m
B6

Fig. 5

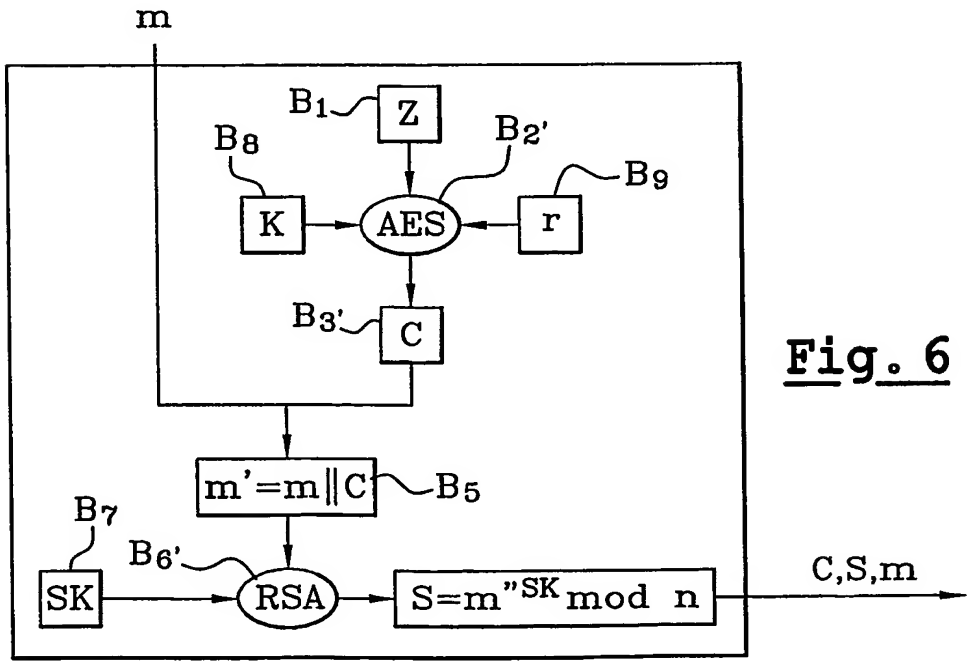

m
B1
Z
B8
B2'
B9
K
AES
r
B3'
C
m'=m||C
B5
B7
B6'
SK
RSA
S=m"SK mod n
C,S,m

Fig. 6

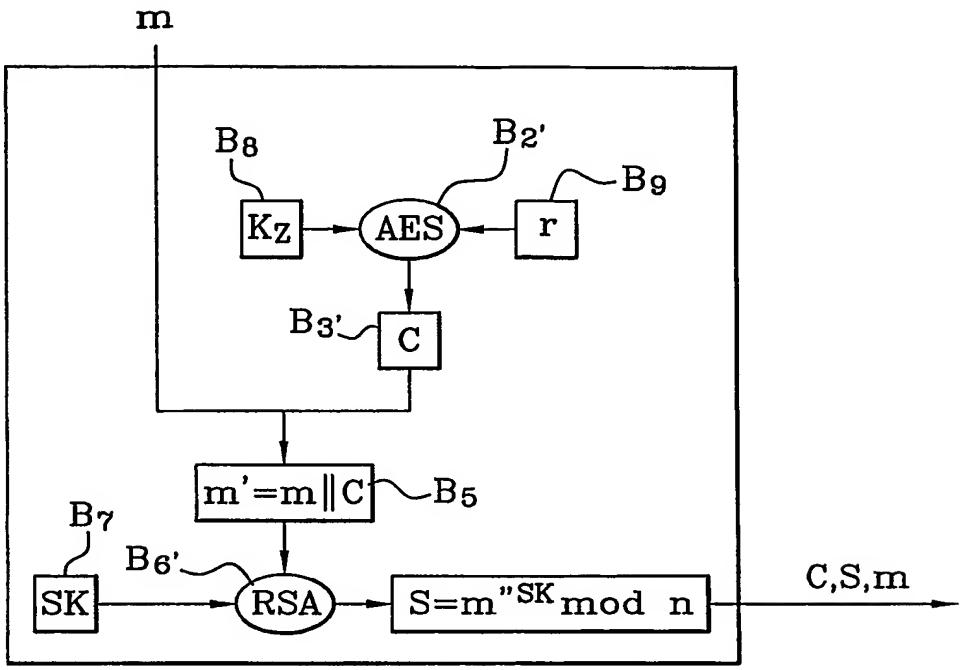

m
B8
B2'
B9
Kz
AES
r
B3'
C
m'=m||C
B5
B7
B6'
SK
RSA
S=m"SK mod n
C,S,m

Fig. 7

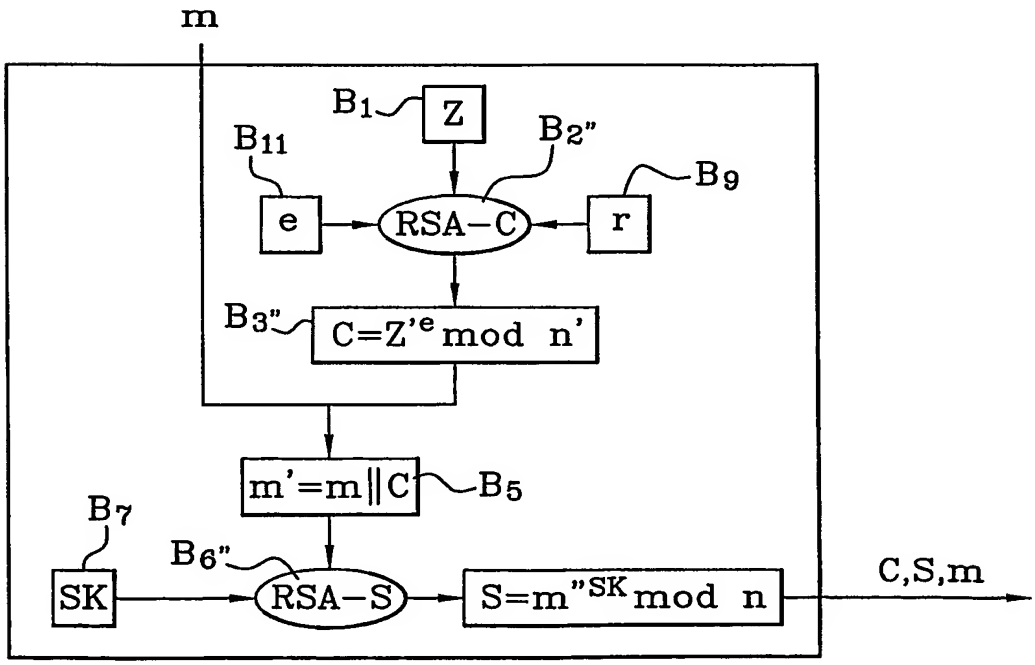

m
B1
Z
B11
B2"
B9
e
RSA-C
r
B3"
C=Z'e mod n'
m'=m||C
B5
B7
B6"
SK
RSA-S
S=m"SK mod n
C,S,m

Fig. 8